PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF RECEIPT OF RECORD COPY

(PCT Rule 24.2(a))

To:

KUSANO, Takashi
Sagami Building
2-21, Shinjuku 4-chome
Shinjuku-ku, Tokyo 160-0022
JAPON

Date of mailing (day/month/year)	**IMPORTANT NOTIFICATION**
08 November 1999 (08.11.99)	
Applicant's or agent's file reference	**International application No.**
11F024	PCT/JP99/02924

The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

NIPPON TELEGRAPH AND TELEPHONE CORPORATION (for all designated States except US)
MORIAI, Shiho et al (for US)

International filing date	:	01 June 1999 (01.06.99)
Priority date(s) claimed	:	02 June 1998 (02.06.98)
Date of receipt of the record copy by the International Bureau	:	14 June 1999 (14.06.99)
List of designated Offices	:	

EP :AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE
National :CA,US

ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- [X] time limits for entry into the national phase
- [X] confirmation of precautionary designations
- [X] requirements regarding priority documents

A copy of this Notification is being sent to the receiving Office and to the International Searching Authority.

CORRECTED VERSION

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer:
Shinji GARASHI

Telephone No. (41-22) 338.83.38

特　許　協　力　条　約

PCT

EP　US　国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　'11F024	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ９９／０２９２４	国際出願日 （日.月.年）　０１．０６．９９	優先日 （日.月.年）　０２．０６．９８
出願人（氏名又は名称） 日本電信電話株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　3　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ｉ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　1　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９９／０２９２４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int.Cl⁶　Ｈ０４Ｌ　９／０６
　　Ｇ０９Ｃ　１／００

Ｂ．　調査を行った分野
調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int.Cl⁶　Ｇ０９Ｃ　１／００　－　５／００
　　Ｈ０４Ｋ　１／００　－　３／００
　　Ｈ０４Ｌ　９／００　－　９／３８

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	盛合志帆“差分/線形/高階差分/補間攻撃に対して強いS-boxの一構成法”１９９８年暗号と情報セキュリティシンポジウム，（１９９８年１月），SCIS'98-2.2.C	1-5, 9, 11, 12, 27, 29-30 6-8, 10, 13-26 28
X Y	浜田猛，横山尚史，島田徹，金子敏信“DES暗号に対するpartitioning解析に関する一考察”１９９８年暗号と情報セキュリティシンポジウム，（１９９８年１月），SCIS'98-2.2.A	1, 3, 4, 9-12, 27-30 2, 5-8, 13-26

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１２．０８．９９	２４.０８.９９

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	丸山　高政	５Ｗ	９５７０
	電話番号　０３－３５８１－１１０１　内線　３５７６		

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９９／０２９２４

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	Susan K. Kangford and Martin E. Hellman, "Differential-Linear Cryptanalysis,"	1-5, 9-12, 27-30
Y	Lecture Notes in Computer Science, Vol. 839, (1994), p. 17-25	6-8, 13-26
Y	櫻井幸一「暗号理論の基礎」共立出版，（１９９６年），p. 69-72，特に72ページ参照	6-8, 19, 26
A	神田雅透，高嶋洋一，松本勉"少数のS-boxを用いたラウンド関数の構成法について（その２）"１９９８年暗号と情報セキュリティシンポジウム，（１９９８年１月），SCIS'98-2.2.D	6-8, 13-26
ＰＸ	盛合志穂，青木和麻呂，神田雅透，高嶋洋一，太田和夫"既知のブロック暗号攻撃に対する安全性を考慮したS-boxの構成法"電子情報通信学会技術研究報告，Vol. 98, No. 227,（１９９８年７月３０日），p. 25－32（ISEC98-13）	1-30

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING SUBMISSION OR TRANSMITTAL OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

KUSANO, Takashi
Sagami Building
2-21, Shinjuku 4-chome
Shinjuku-ku, Tokyo 160-0022
JAPON

Date of mailing (day/month/year) 08 November 1999 (08.11.99)	
Applicant's or agent's file reference 11F024	**IMPORTANT NOTIFICATION**
International application No. PCT/JP99/02924	International filing date (day/month/year) 01 June 1999 (01.06.99)
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 02 June 1998 (02.06.98)
Applicant NIPPON TELEGRAPH AND TELEPHONE CORPORATION et al	

1. The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).

2. This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.

3. An **asterisk(*)** appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

4. The **letters "NR"** appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
02 June 1998 (02.06.98)	10/153066	JP	16 July 1999 (16.07.99)

CORRECTED VERSION

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer
S. Igarashi
Shinji IGARASHI

Telephone No. (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING SUBMISSION OR TRANSMITTAL OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

KUSANO, Takashi
Sagami Building
2-21, Shinjuku 4-chome
Shinjuku-ku, Tokyo 160-0022
JAPON

Date of mailing (day/month/year) 05 August 1999 (05.08.99)	
Applicant's or agent's file reference 11F024	**IMPORTANT NOTIFICATION**
International application No. PCT/JP99/02924	International filing date (day/month/year) 01 June 1999 (01.06.99)
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 02 June 1998 (02.06.98)
Applicant NIPPON TELEGRAGH AND TELEPHONE CORPORATION et al	

1. The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).

2. This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.

3. An **asterisk(*)** appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

4. The **letters "NR"** appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
02 June 1998 (02.06.98)	10/153066	JP	16 July 1999 (16.07.99)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer

Carlos Naranjo

Telephone No. (41-22) 338.83.38

002771921

Form PCT/IB/304 (July 1998)

PATENT COOPERATION TREATY

For our reference

From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:
KUSANO, Takashi
Sagami Building
2-21, Shinjuku 4-chome
Shinjuku-ku, Tokyo 160-0022
JAPON

Date of mailing (day/month/year) 09 December 1999 (09.12.99)	
Applicant's or agent's file reference 11F024	**IMPORTANT NOTICE**
International application No. PCT/JP99/02924	**International filing date** (day/month/year) 01 June 1999 (01.06.99)
Priority date (day/month/year) 02 June 1998 (02.06.98)	
Applicant NIPPON TELEGRAPH AND TELEPHONE CORPORATION et al	

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
   EP,US

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
   CA

   The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
   09 December 1999 (09.12.99) under No. WO 99/63706

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, **a demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer
J. Zahra

Telephone No. (41-22) 338.83.38

PCT REQUEST 11f024

Draft (**NOT** for submission) - printed on 28.01.2000 10:49:02 AM

0 0-1	**For receiving Office use only** International Application No.	PCT/JP99/02924
0-2	International Filing Date	01 June 1999
0-3	Name of receiving Office and "PCT International Application"	
0-4 0-4-1	**Form - PCT/RO/101 PCT Request** Prepared using	**PCT-EASY Version 2.~~90~~** 83 **(updated ~~15.12~~.1999)**
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	01.03.
0-6	**Receiving Office (specified by the applicant)**	**Japanese Patent Office (RO/JP)**
0-7	**Applicant's or agent's file reference**	**11f024**
I	**Title of invention**	**APPARATUS AND METHOD FOR EVALUATING RANDOMNESS OF FUNCTIONS, RANDOM FUNCTION GENERATING APPARATUS AND METHOD, AND RECORDING MEDIUM HAVING RECORDED THEREON PROGRAMS FOR IMPLEMENTING THE METHODS**
II II-1 II-2 II-4 II-5 II-6 II-7 II-8 II-9	**Applicant** This person is: Applicant for Name Address: State of nationality State of residence Telephone No. Facsimile No.	**applicant only** **all designated States except US** **NIPPON TELEGRAPH AND TELEPHONE CORPORATION** **19-2, Nishi-Shinjuku 3-chome, Shinjuku-ku, Tokyo 163-8019 Japan** **JP** **JP** **03-5353-4343** **03-5353-5518**
III-1 III-1-1 III-1-2 III-1-4 III-1-5 III-1-6 III-1-7	**Applicant and/or inventor** This person is: Applicant for Name (LAST, First) Address: State of nationality State of residence	**applicant and inventor** **US only** **MORIAI, Shiho** **1-21-1-701, Kamioooka-higashi, Kounan-ku, Yokohama-shi, Kanagawa 233-0001 Japan** **JP** **JP**

PCT REQUEST 11f024

Draft (**NOT** for submission) - printed on 28.01.2000 10:49:02 AM

III-2	**Applicant and/or inventor**	
III-2-1	This person is:	applicant and inventor
III-2-2	Applicant for	US only
III-2-4	Name (LAST, First)	AOKI, Kazumaro
III-2-5	Address:	4-22-1-A-503, Kamariya-higashi, Kanazawa-ku, Yokohama-shi, Kanagawa 236-0042 Japan
III-2-6	State of nationality	JP
III-2-7	State of residence	JP
III-3	**Applicant and/or inventor**	
III-3-1	This person is:	applicant and inventor
III-3-2	Applicant for	US only
III-3-4	Name (LAST, First)	KANDA, Masayuki
III-3-5	Address:	D-401, 9-2-12, Sugita, Isogo-ku, Yokohama-shi, Kanagawa 235-0033 Japan
III-3-6	State of nationality	JP
III-3-7	State of residence	JP
III-4	**Applicant and/or inventor**	
III-4-1	This person is:	applicant and inventor
III-4-2	Applicant for	US only
III-4-4	Name (LAST, First)	TAKASHIMA, Youichi
III-4-5	Address:	2-30-21, Kamariya-nishi, Kanazawa-ku, Yokohama-shi, Kanagawa 236-0046 Japan
III-4-6	State of nationality	JP
III-4-7	State of residence	JP
III-5	**Applicant and/or inventor**	
III-5-1	This person is:	applicant and inventor
III-5-2	Applicant for	US only
III-5-4	Name (LAST, First)	OHTA, Kazuo
III-5-5	Address:	2-10-34, Yamanone, Zushi-shi, Kanagawa 249-0002 Japan
III-5-6	State of nationality	JP
III-5-7	State of residence	JP

PCT REQUEST 11f024

Draft (**NOT** for submission) - printed on 28.01.2000 10:49:02 AM

IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name (LAST, First)	KUSANO, Takashi
IV-1-2	Address:	Sagami Building, 2-21, Shinjuku 4-chome, Shinjuku-ku, Tokyo 160-0022 Japan
IV-1-3	Telephone No.	03-3350-6456
IV-1-4	Facsimile No.	03-5379-7396
IV-2	**Additional agent(s)**	additional agent(s) with same address as first named agent
IV-2-1	Name(s)	INAGAKI, Minoru
V	**Designation of States**	
V-1	Regional Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and any other State which is a Contracting State of the European Patent Convention and of the PCT
V-2	National Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	CA US
V-5	**Precautionary Designation Statement** In addition to the designations made under items V-1, V-2 and V-3, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except any designation(s) of the State(s) indicated under item V-6 below. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.	
V-6	**Exclusion(s) from precautionary designations**	NONE
VI-1	**Priority claim of earlier national application**	
VI-1-1	Filing date	02 June 1998 (02.06.1998)
VI-1-2	Number	153066/98
VI-1-3	Country	JP
VI-2	**Priority document request** The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s):	VI-1

PCT REQUEST 11f024

Draft (**NOT** for submission) - printed on 28.01.2000 10:49:02 AM

VII-1	**International Searching Authority Chosen**	Japanese Patent Office (JPO) (ISA/JP)	
VIII	**Check list**	number of sheets	electronic file(s) attached
VIII-1	Request	~~4~~ 5	-
VIII-2	Description	18	-
VIII-3	Claims	13	-
VIII-4	Abstract	1	- 11f024.txt
VIII-5	Drawings	2	-
VIII-7	TOTAL	~~38~~ 39	
	Accompanying items	paper document(s) attached	electronic file(s) attached
VIII-8	Fee calculation sheet	✓	-
VIII-9	Separate signed power of attorney	✓	-
VIII-16	PCT-EASY diskette	-	diskette
VIII-17	Other (specified):	Request for mailing Priority Document	-
VIII-18	**Figure of the drawings which should accompany the abstract**	1	
VIII-19	**Language of filing of the international application**	Japanese	
IX-1	**Signature of applicant or agent**		
IX-1-1	Name (LAST, First)	KUSANO, Takashi (Seal)	
IX-2	**Signature of applicant or agent**		
IX-2-1	Name (LAST, First)	INAGAKI, Minoru (Seal)	

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	
10-2	**Drawings:**	
10-2-1	Received	
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/JP
10-6	**Transmittal of search copy delayed until search fee is paid**	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	

世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6
H04L 9/06, G09C 1/00

A1

(11) 国際公開番号 WO99/63706

(43) 国際公開日 1999年12月9日(09.12.99)

(21) 国際出願番号 PCT/JP99/02924

(22) 国際出願日 1999年6月1日(01.06.99)

(30) 優先権データ
特願平10/153066 1998年6月2日(02.06.98) JP

(71) 出願人（米国を除くすべての指定国について）
日本電信電話株式会社(NIPPON TELEGRAPH AND TELEPHONE CORPORATION)[JP/JP]
〒163-8019 東京都新宿区西新宿三丁目19番2号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
盛合志帆(MORIAI, Shiho)[JP/JP]
〒233-0001 神奈川県横浜市港南区上大岡東1-21-1-701 Kanagawa, (JP)
青木和麻呂(AOKI, Kazumaro)[JP/JP]
〒236-0042 神奈川県横浜市金沢区釜利谷東4-22-1-A-503 Kanagawa, (JP)
神田雅透(KANDA, Masayuki)[JP/JP]
〒235-0033 神奈川県横浜市磯子区杉田9-2-12 D-401 Kanagawa, (JP)
高嶋洋一(TAKASHIMA, Youichi)[JP/JP]
〒236-0046 神奈川県横浜市金沢区釜利谷西2-30-21 Kanagawa, (JP)
太田和夫(OHTA, Kazuo)[JP/JP]
〒249-0002 神奈川県逗子市山の根2-10-34 Kanagawa, (JP)
(74) 代理人
草野 卓, 外(KUSANO, Takashi et al.)
〒160-0022 東京都新宿区新宿四丁目2番21号 相模ビル Tokyo, (JP)

(81) 指定国 CA, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

添付公開書類
国際調査報告書

(54)Title: **DEVICE AND METHOD FOR EVALUATING RANDOMNESS OF FUNCTION, DEVICE AND METHOD FOR GENERATING RANDOM FUNCTION, AND RECORDED MEDIUM ON WHICH PROGRAMS FOR IMPLEMENTING THESE METHODS ARE RECORDED**

(54)発明の名称 関数のランダム性評価装置及び評価方法、ランダム関数生成装置及び生成方法、及びこれら方法を実施するプログラムを記録した記録媒体

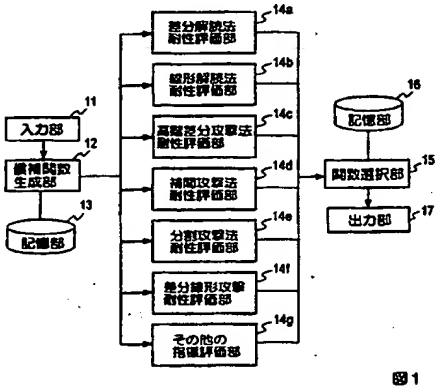


図1

11 ... INPUT UNIT
12 ... FUNCTION CANDIDATE GENERATING UNIT
13 ... STORAGE UNIT
14a ... DIFFERENTIAL DECODING METHOD RESISTANCE EVALUATING UNIT
14b ... LINEAR DECODING METHOD RESISTANCE EVALUATING UNIT
14c ... HIGH-ORDER DIFFERENTIAL ATTACK METHOD RESISTANCE EVALUATING UNIT
14d ... INTERPOLATION ATTACK METHOD RESISTANCE EVALUATING UNIT
14e ... DIVISION ATTACK METHOD RESISTANCE EVALUATING UNIT
14f ... DIFFERENTIAL LINEAR ATTACK RESISTANCE EVALUATING UNIT
14g ... OTHER INDICES EVALUATING UNIT
15 ... FUNCTION SELECTING UNIT
16 ... STORAGE UNIT
17 ... OUTPUT UNIT

(57) Abstract

To evaluate the randomness of an S-box, the indices of strength against the high-order differential attack method, interpolation attack method, division attack method, and differential linear attack method and the necessary conditions under which the indices have resistances to decoding methods are determined. Whether or not each of function candidates meets part or all of the conditions is checked, and candidates which meet the part or all of the conditions are selected, as necessary. For each selected candidate, the resistance to at least either the differential decoding method or the linear decoding method is evaluated, and function candidates having strong resistances to at least one of them can be selected, as necessary.

(57)要約

S-box のランダム性評価において、高階差分攻撃法、補間攻撃法、分割攻撃法、差分線形攻撃法に対する強度指標とそれらの強度指標が各解読法に対する耐性をもつための必要条件を設定し、候補となる関数群について上記の一部または全ての条件が満たされるかどうかを評価し、必要に応じて上記の一部または全ての条件が満たされるものを選ぶ。更に、この選ばれたものに対し差分解読法、線形解読法の少くとも一方に対して耐性を評価し、必要に応じて少なくとも一方に対して耐性の強いものを選んでもよい。

明細書

関数のランダム性評価装置及び評価方法、ランダム関数生成装置及び生成方法、及びこれら方法を実施するプログラムを記録した記録媒体

技術分野

この発明は、例えば暗号装置等へ適用され、入力に対する出力が不規則に生成され、その動作を解析することが困難であるような関数を得るために、いくつかのランダム性指標を満たすかどうかを評価する装置及び方法、ランダム性指標を満たすと評価されたランダム関数を生成する装置及び方法、及びこれらの方法を実施するプログラムを記録した記録媒体に関する。

従来の技術

データを秘匿するためには暗号化技術が有効である。暗号化の方法は秘密鍵暗号方式と公開鍵暗号方式がある。一般に公開鍵暗号技術の方が安全性の証明技術の研究が進んでいるので、安全性の限界を知りつつ利用することができる。しかし、秘密鍵暗号については安全性の証明技術は確立されておらず、暗号攻撃が発見されると、その都度、個別に対処する必要が生じる。

高速かつ安全な秘密鍵暗号を構成するために、暗号化対象のデータを適当な長さのブロックに分割し、そのブロック毎に暗号化する方法をブロック暗号と呼ぶ。通常ブロック暗号は暗号学的にあまり強くない関数を、平文に対し複数回繰り返し適用することにより安全性を高めている。この、あまり強くない関数をＦ関数と呼ぶ。

Ｆ関数の構成要素として、S-box と呼ばれる、入力に対する出力が不規則に生成され、その動作を解析することが困難であるようなランダム関数を用いることが一般的となっている。入出力関係が一意であるランダム関数機能を有するS-box は、その入出力関係を表として有するＲＯＭにより構成することによりランダム関数演算自体の複雑さに無関係に、入力に対し一定かつ高速に出力を生成することができる。S-box は代表的な例としてDES(Data Encryption Standard) で採用されて以来、その安全性や設計法について研究されてきた。従来は、S-box を構成する際に、安全性の根拠として、例えば、暗号化したデータの各ビットの０，１の出現確率が統計的に1/2 となる程度のことしか考えられておらず、ブロック暗号の理論的な安

全性の根拠として不十分であった。

実際、上記の基準を満たすブロック暗号に対する攻撃法として、差分解読法が文献「E. Biham, A. Shamir: "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, Vol. 4, No. 1, pp. 3-72」で、線形解読法が文献「M. Matsui: "Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology-EUROCRYPT'93(Lecture Notes in Computer Science 765), pp. 386-397, Springer-Verlag, 1994」で提案され、多くのブロック暗号がこれらの解読法により解読できることがわかり、安全性の基準の見直しが必要となった。

差分解読法や線形解読法が提案されてからブロック暗号にはこれらの解読法に対して強いことが要求されるようになった。そこで、これらの解読法に対して耐性があることを示す指標として、それぞれ最大平均差分確率や最大平均線形確率が文献「M. Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis," D. Gollmann, editor, Fast Software Encryption, Third International Workshop, Cambridge, UK, February 1996, Proceedings, Vol. 1039 of Lecture Notes in Computer Science, pp. 205-218, Springer-Verlag, Berlin, Heidelberg, New York, 1996」で提案された。これらの指標は小さいほどそれぞれの解読法に対する耐性があることが示されている。

更に近年、差分解読法や線形解読法に対する耐性のある暗号でも、これ以外の解読法によって解読されることが指摘され、更に安全性の基準の見直しが必要となった。具体的には、文献「T. Jakobsen, L. R. Knudsen: "The Interpolation Attack on Block Cipher," Fast Software Encryption Workshop(FSE4)(Lecture Notes in Computer Science 1267), pp. 28-40, Springer Verlag, 1997」において、差分解読法や線形解読法に対する耐性のある暗号でも、高階差分攻撃や補間攻撃によって解読される暗号があることが示された。

更に高階差分攻撃や補間攻撃以外にも文献「C. Harpes, J. L. Massey: "Partitioning Cryptanalysis," Fast Software Encryption Workshop(FSE4)(Lecture Notes in Computer Scinece 1267), pp. 13-27, Springer Verlag, 1997」において線形

解読法を一般化した分割攻撃が提案され、この攻撃に対しても十分な耐性があることを保証することが必要となっている。

差分解読法、線形解読法に対する安全性を保証する技術が、一部のブロック暗号の構成法に対して確立しているのに対して、高階差分攻撃、補間攻撃、分割攻撃に対して完全に耐性があることを保証する技術は現時点では確立していない。即ち、暗号がこれらの攻撃に対して安全であるためにランダム関数、いわゆるS-box が満たすべき必要十分条件は明らかになっていない。

しかし、S-box を設計する上で、これらの攻撃法に対しても十分な強度をもつようにすることは重要な課題である。S-box に対するこれらの攻撃は入出力関係に何らかの偏りを見つけ、それを利用することに基づいている。従って、攻撃に対し耐性のあるS-box を設計することは、入出力関係に偏りの少ないもの、即ちランダムなものを設計することである。従って、攻撃に対するS-box の耐性を評価することはS-box のランダム性を評価することである。

そこで、この発明の一目的は、上記の各攻撃法に対し、その攻撃法に対する強度と深く関わる指標を見い出し、その指標が（各攻撃に対して強いことを保証する必要十分条件を満たさないまでも、）各攻撃に対して耐性をもつための必要条件を示し、それに基づいて関数のランダム性を評価する性評価装置とその評価方法及びその方法をプログラムとして記録した記録媒体を提供することにある。更に、この発明の他の目的はこれらの強度指標を満たすランダム関数の生成装置と生成方法及びその方法をプログラムとして記録した記録媒体を提供することにある。

発明の開示

この発明による関数のランダム性評価装置及び評価方法においては、

評価すべき関数の各出力ビットを入力ビットに関するブール多項式で表現したときの次数の最小値を求めてその最小値が大きいほど高階差分攻撃法に対する耐性が大であると評価する処理と、

上記評価すべき関数に対し、鍵ｋを固定して入力をｘとしたとき、素数ｐ又はｐのべき乗個の要素からなるガロア体上の多項式を用いて出力ｙを$y=f_k(x)$と表現して、上記多項式の項数を求め、その項数が大であるほど補間攻撃法に対する耐性

が大であると評価する処理と、

上記評価すべき関数の全ての入力とそれらに対応する出力をそれぞれ入力部分集合及び出力部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との関係の、その平均的対応関係に対する偏りを求めて、分割攻撃法に対する耐性を評価する処理と、

評価すべき関数S(x)について入力差分Δx と出力マスク値Γy の全ての組に対し(S(x)+S(x+Δx))と出力のマスク値Γy との内積が１であるｘの個数を求めて差分線形攻撃法に対する耐性を評価する処理、

の少なくとも１つを実行する。

この発明によるランダム関数生成装置及び生成方法においては、代数構造の異なる複数の関数を組合わせた関数であり複数のパラメータを有する候補関数群を生成し、上記各候補関数群のそれぞれについて、解読攻撃に対する耐性を評価し、耐性の強い候補関数群を選出する。

図面の簡単な説明

図１はこの発明によるランダム関数生成装置、関数のランダム性評価装置の機能的構成例を示すブロック図。

図２はこの発明によるランダム関数生成装置の基本構成の例を示すブロック図。

図３はこの発明によるランダム関数生成装置の実施例の処理手順の例を示す流れ図。

発明を実施するための最良の形態

この発明の第１の観点による実施例

図１にこの発明によるランダム関数生成装置、関数のランダム性評価装置の実施例の機能構成を示す。入力部１１により、候補関数生成部１２において候補関数を生成するのに必要なデータとそのパラメータなどが入力され、候補関数生成部１２において、入力部１１の入力に応じた候補関数が生成され、そのパラメータ値と入力値とこれらにもとづく演算結果（出力値）とが記憶部１３に記憶される。記憶部１３に記憶された各種データが読出され、差分解読法耐性評価部14a 、線形解読法

耐性評価部14b 、高階差分攻撃法耐性評価部14c 、補間攻撃法耐性評価部14d 、分割攻撃法耐性評価部14e 、差分線形攻撃法耐性評価部14f 、その他の指標評価部14g でそれぞれ耐性評価、指標評価などがなされる。その各結果にもとづき、耐性の強い候補関数が関数選択部１５で選択され、記憶部１６に記憶され、所要のものが出力部１７から出力される。

この発明による関数がランダム性評価装置においては、入力部１１から評価されるべき関数が各評価部14a～14gに入力されて、ランダム性評価が行われる。

以下に差分解読法、線形解読法、高階差分攻撃法、補間攻撃法、分割攻撃法、差分線形攻撃法に対する強度指標とそれらの強度指標が各解読法に対する耐性をもつための必要条件を述べる。以下ではｎ，ｍを任意の自然数とし、S-box （ランダム関数）としてｎビット入力、ｍビット出力の関数Ｓ：$GF(2)^n \rightarrow GF(2)^m$を考える。$GF(2)^n$は全てのｎビットデータの集合を示す。

(a) 差分解読法に対する耐性をもつための必要条件

S-box の差分解読法に対する耐性を示す指標として差分攻撃指標を定義し、その測定方法を述べ、差分解読法に対する耐性をもつための必要条件を示す。差分解読法では、S-box の２つの入力の差分（入力差分値）に対する出力の差分（出力差分値）を観測し、大きな偏りがある場合に、これを利用して暗号全体の解読につなげることができる。

S-box の入力をｘ、２つの入力の差分値をΔx 、その２つの入力に対応する２つの出力の差分値をΔy 、S-box の関数をＳ、入力ｘに対するS-box の出力ｙをy=S(x)とすると、任意の入力差分値Δx と、任意の出力差分値Δy に対して、全てのｎビット入力ｘのうち、次式(1)

$$S(x)+S(x+\Delta x)=\Delta y \qquad (1)$$

を満たすｘの個数を$\delta_s(\Delta x, \Delta y)$とする。但し、通常、“＋”はビット毎の排他的論理和(XOR) で定義される。文献「X. Lai, J. L. Massey, and S. Murphy, ″Markov Ciphers and Differential Cryptanalysis,″ In D. W. Davies, editor, Advances in Cryptology-EUROCRYPT '91, Volume 547 of Lecture Notes in Computer Science, pp. 17-38. Springer-Verlag, Berlin, Heidelberg, New York, 1991」 で

述べられているように、差分演算の代わりに一般的な逆元がある任意の二項演算を用いることができるが、これらを含め、差分解読法と呼ぶ。差分解読法では、任意の２つの入力間の演算結果と、それに対応する２つの出力間の演算結果の関係に偏りが生じることを見つけ、それを利用して解読を行う。

与えられたΔx とΔy の組に対し式(1) を満足するｘの個数$\delta_s(\Delta x, \Delta y)$ は次式(2)

$$\delta_s(\Delta x, \Delta y) = \#\{x \in GF(2)^n \mid S(x) + S(x+\Delta x) = \Delta y\} \qquad (2)$$

のように表現される。但し、＃{ｘ｜条件式} は条件式を満たすｘの個数とする。入力差分値として０を除く全てのｎビットデータΔx と出力差分値として全てのｍビットデータΔy に対して、式(2) より$\delta_s(\Delta x, \Delta y)$ を計算することができる。このうち最も大きい値をとるΔx とΔy の組合せが差分解読法における脆弱点となるため、$\delta_s(\Delta x, \Delta y)$ の最大値が小さいほど差分解読法に対する耐性が大きいということになる。よって次式(3)

$$\Delta_s = \max \delta_s(\Delta x, \Delta y) \qquad (3)$$

で示される差分解読指標Δ_s が小さいことが差分解読法に対して耐性をもつための必要条件となる。式(3) は$\Delta x \neq 0$、Δy の全組合せの中か最大のδ_s を選び、Δ_s の値とすることを表す。

(b) 線形解読法に対する耐性をもつための必要条件

S-box の線形解読法に対する耐性を示す指標として線形攻撃指標を定義し、その測定方法を述べ、線形解読法に対する耐性をもつための必要条件を示す。

線形解読法では、S-box の入力値と出力値のビット単位での任意の線形和（排他的論理和）を観測し、大きな偏りがある場合に、これを利用して暗号全体の解読につなげることができる。

S-box の入力をｘ、入力マスク値をΓx 、出力マスク値をΓy とすると、ある入力マスク値Γx と出力マスク値Γy に対して、次式(4)

$$\lambda_s(\Gamma x, \Gamma y) = |2 \times \#\{x \in GF(2)^n \mid x \cdot \Gamma x = S(x) \cdot \Gamma y\} - 2^n| \qquad (4)$$

で定義される$\lambda_s(\Gamma x, \Gamma y)$ が計算できる。但し、通常、“・”は内積で定義され

る。x・Γxの意味は、マスク値Γx中の“0”に対応するx中のビット値は無視し、“1”に対応するx中のビット値のみを有効として、それらの和をとることを表わす。即ち、x・Γx＝Σxi（ΣはΓx 中の第iビットが“1”の総和）但しx＝($x_{n-1}, \cdots, x_0$）とする。y・Γyの意味も同様である。従って、式(4) は与えられたマスク値の組（Γx, Γy）に対し、nビットの全ての入力x （2^n個ある）のうち、x・Γx＝S(x)・Γy を満足するxの個数の２倍から2^nを減算して得た値の絶対値を表している。

入力マスク値としてnビットデータΓx と、出力マスク値として0を除くmビットデータΓy の全ての組に対して、それぞれ式(4) よりλs(Γx, Γy)を計算することができる。このうちλs(Γx, Γy)が最も大きい値をとるΓx とΓy の組が線形解読法における脆弱点となるため、λs(Γx, Γy) の最大値が小さいほど線形解読法に対する耐性が大きいということになる。よって次式(5)

$$\Lambda_s = \max \lambda_s(\Gamma x, \Gamma y) \qquad (5)$$

で示される線形解読指標Λs が小さいことが線形解読法に対して耐性をもつための必要条件となる。

式(5) はΓx , Γy≠0の全ての組合わせの中からλs(Γx, Γy)の最大値を選び、Λs とすることを表す。

(c) 高階差分攻撃法に対する耐性をもつための必要条件

S-box の高階差分攻撃法に対する耐性を示す指標として高階差分攻撃指標を定義し、その測定方法を述べ、高階差分攻撃法に対する耐性をもつための必要条件を示す。

高階差分攻撃法とは、暗号化途中の中間出力を入力に関して高階差分をとると、鍵によらない定数になることを利用した攻撃法である。暗号化途中の任意の中間データの任意のビットは、入力に関するブール多項式で表現できる。即ち、例えばある中間データのあるビットy_jは、Nビット入力xに関するブール多項式で例えば

$$y_j = x_0 + x_1x_3 + x_0x_2x_3 + \ldots + x_1x_4x_5x_6\cdots x_N \qquad (6)$$

のように表すことができる。そのブール多項式の次数がdであった時、出力のd+1階差分（例えば2^{d+1}個の出力の排他的論理和）をとると、その結果は鍵によらな

い定数になることから、これまでに、ブール多項式の次数が低い暗号に対する攻撃が前記文献Ａで報告されている。

Ｆ関数のブール多項式表現の次数が低ければ、Ｆ関数の繰り返し回数が十分多くないと暗号全体のブール多項式表現の次数も高くならず、解読される危険性が高い。よって、Ｆ関数の構成要素であるS-box のブール多項式表現の次数も高いことが、Ｆ関数の繰り返し回数を増やすことなくその暗号が高階差分攻撃に対して安全にするための必要条件といえる。

S-box $S : GF(2)^n \rightarrow GF(2)^m$; $x \mapsto S(x)$

に対し、

$$y = S(x), \tag{7a}$$

$$x = (x_{n-1}, x_{n-2}, \cdots, x_0) \in GF(2)^n, \tag{7b}$$

$$y = (y_{m-1}, y_{m-2}, \cdots, y_0) \in GF(2)^m \tag{7c}$$

とする。また、変数集合$X = \{x_{n-1}, x_{n-2}, \cdots, x_0\}$を定義する。この時、$y_i = S_i(x)$なるブール関数

$$S_i : GF(2)^n \rightarrow GF(2) ; \quad x \mapsto S_i(x) \tag{8}$$

を定義し、変数集合Ｘに関するブール関数S_i（$0 \leqq i \leqq m-1$）の次数を $deg_x S_i$とする。以下のように $deg_x S_i$（$0 \leqq i \leqq m-1$）の最小値を$deg_x S$とし、これが高階差分攻撃指標となる。

$$deg_x S = \min (deg_x S_i) \tag{9}$$

min は$0 \leqq i \leqq m-1$を条件とする。

高階差分攻撃に対して安全であるためにS-box が満たすべき必要条件は、$deg_x S$が大きい値をもつことである。Ｓが全単射（即ち、入出力関係が両方向で一意に決まる）であれば、$deg_x S$の最大値はn－1であることが知られている。

(d) 補間攻撃法に対する耐性をもつための必要条件

S-box の補間攻撃法に対する耐性を示す指標として補間攻撃指標を定義し、その測定方法を述べ、補間攻撃法に対する耐性をもつための必要条件を示す。

補間攻撃の原理は次の通りである。鍵ｋを固定した時、暗号文ｙは、平文ｘについてのGF(q) 上多項式$f_k(x)$ を用いて例えば次式

$$y = f_k(x) = c_{q-1}x^{q-1} + c_{q-2}x^{q-2} + \ldots + c_j x^j + \ldots + c_1 x^1 + c_0 x^0 \qquad (10)$$

のように表すことができる。但し、qは素数または素数のべき乗である。多項式$f_k(x)$に含まれる係数が非ゼロのxについての項数がcである時、異なるc組の平文とそれに対する暗号文の組$(x_i, y_i)(i=1,\ldots,c)$が与えられれば、ラグランジェ補間公式などにより、$f_k(x)$を構成することができる。これにより、任意の平文xに対する暗号文を得ることができる。

多項式$f_k(x)$に含まれる項数が多いほど、GF(q)上多項式表現$f_k(x)$を用いた補間攻撃に必要な平文と暗号文の組は多くなり、攻撃は困難または不可能となる。

S-boxのGF(q)上多項式表現に含まれる項数が少ないと、暗号全体のGF(q)上多項式表現に含まれる項数が少なくなる可能性がある。もちろん、S-boxのGF(q)上多項式表現に含まれる項数が多くても、暗号全体を構成する上で項が打ち消し合い、暗号全体のGF(q)上多項式表現に含まれる項数が少なくならないよう注意する必要はあるが、これは暗号構成法に関することであり、S-boxの補間攻撃指標としてはGF(q)上多項式表現に含まれる項数が多いことが補間攻撃法に対する耐性をもつための必要条件となる。S-boxの関数SのGF(q)上多項式表現に含まれる項数を$\mathrm{coeff}_q S$とし、これをGF(q)上多項式表現を利用する補間攻撃の攻撃指標とする。

補間攻撃は想定されるqとして取りうる場合の数だけ攻撃が存在するので、なるべく多くのGF(q)上多項式表現に対してその項数$\mathrm{coeff}_q S$を計算し、それらが小さい値をとらないことを確認することが望ましい。

(e) 分割攻撃法に対する耐性をもつための必要条件

S-boxの分割攻撃法に対する耐性を示す指標として分割攻撃指標を定義し、その測定方法を述べ、分割攻撃法に対する耐性をもつための必要条件を示す。分割攻撃法では、平文集合全体のある部分集合と暗号文集合全体のある部分集合に成り立つ何らかの指標を観測し、大きな偏りが見い出される場合に、これを利用して暗号全体の解読につなげることができる。この「何らかの指標Ⅰ」としては、文献「C. Harpes, J. L. Massey : "Partitioning Cryptanalysis," Fast Software Encryption Workshop (FSE4) (Lecture Notes in Computer Science 1267), pp. 13-27, Spri

nger Verlag, 1997」ではpeak imbalanceとsquared Euclidean imbalance が例として挙げられている。

文献「浜出　猛，横山尚史，島田　徹，金子敏信：「ＤＥＳ暗号に対するpartitioning cryptanalysis of DES, 1998年暗号と情報セキュリティシンポジウム予稿集（SCIS'98-2.2.A)」において、DES 暗号のS-box の入出力集合に対して観測される偏りを利用して、暗号全体の攻撃に成功していることから、S-box の入出力集合に対して同様に定義された分割攻撃指標が、暗号全体が分割攻撃法に対し耐性をもつための必要条件であることが分かる。

S-box の全入力集合をｕ分割した部分集合をF_0, F_1, ... , F_{u-1}、全出力集合をｖ分割した部分集合をG_0, G_1, ..., G_{v-1} とする。各部分集合に含まれる要素数は全て等しいとする。入力ｘを各部分集合の添字 {0, 1, ..., u-1} に写像する関数ｆを入力の分割関数、出力ｙを部分集合の添え字 {0, 1, ..., v-1} に写像する関数ｇを出力の分割関数と呼ぶ。つまりｘがどの入力部分集合に属するかを示す関数がｆであり、ｙがどの出力部分集合に属するかを決める関数がｇである。分割Ｆ，Ｇをそれぞれ

$$F = \{F_0, F_1, \cdots, F_{u-1}\},$$

$$G = \{G_0, G_1, \cdots, G_{v-1}\}$$

とすると、S-box の分割対(F, G)の偏りI_S(F, G)は次式(11)

$$I_S(F,G) = \frac{1}{u}\sum_{i=0}^{u-1} I(g(S(x)) \mid F(x) = i) \qquad (11)$$

で与えられる。式(11) の右辺における$I(g(S(x)) \mid F(x)=i)$を$I(V)$で表すと、これが前述の「指標Ｉ」であり、C. Harpes 等の前記文献によれば、この指標としてpeak imbalanceを使用する場合は次式

$$I_p(V) = \frac{v}{v-1}\left(\max_{0\le j<v} P[V=j] - \frac{1}{v}\right) \qquad (12)$$

で表される。また、squared Euclidean imbalance を指標として使用する場合は次式

$$I_E(V) = \frac{v}{v-1}\sum_{j=0}^{v-1}\left(P[V=j] - \frac{1}{v}\right)^2 \qquad (13)$$

で表される。P[V=j]はある i (i=0,...,u-1) 番目の入力グループF_iの全入力 x に対応する全出力 y が出力グループG_j (j=0,...,v-1) へ帰属する確率を表し、それぞれの出力グループへの帰属確率の総和は 1 となる。例えばグループF_iの全入力 x (K_i個とする) に対応する全出力 y (K_i個) のうちk_j個の出力がグループG_jに帰属すればグループG_jへの帰属確率はk_j/K_iである。式(12)のpeak imbalance $I_p(V)$は最大帰属確率の平均確率からの偏りを正規化した値を表し、式(13)のEuclidean imbalance $I_E(V)$ は帰属確率の平均からの偏りの２乗和を正規化した値を表している。この指標I_p又はI_Eを式(11)に適用して各種分割対(F, G)について偏り$I_s(F, G)$を求める。分割対は、例えば分割関数 f 及び g の選び方により様々なものを選択する。例えば、分割数 u 、 v も関数 f 、 g により指定されるパラメータの１つである。

式(11)により与えられる指標がS-box の分割攻撃指標であり、0以上１以下の何れかの値をとり、その値と1/2 との差が小さいことが分割攻撃法に対する耐性をもつための必要条件となる。従って、$|I_S(F,G)-1/2|$ の値ができるだけ小さくなる S-box 関数を選ぶ。

(f) 差分線形攻撃法に対する耐性を持つための必要条件

S-box の差分線形攻撃法に対する耐性を示す指標として差分線形攻撃指標を定義し、その測定方法を述べ、差分線形攻撃指標に対する耐性を持つための必要条件を示す。

差分線形攻撃では、S-box の入力差分値と出力差分値の線形和（例えば排他的論理和）を観測し、大きな偏りがある場合に、これを利用して暗号全体の解読につなげることができる。

S-box の入力を x 、入力差分値をΔx 、出力マスク値をΓy とすると、次式

$$\xi_s(\Delta x, \Gamma y) = |2\#\{x \in GF(2)^n \mid [S(x)+S(x+\Delta x)] \cdot \Gamma y = 1\} - 2^n| \quad (14)$$

で定義される$\xi_s(\Delta x, \Gamma y)$が計算できる。ただし、"+" 及び"・"の演算は、それぞれ差分攻撃指標及び線形攻撃指標で使用されているものと同様である。この様にして計算される指標$\xi_s(\Delta x, \Gamma y)$のうち、全ての$\Delta x, \Gamma y$ の組み合わせのうちの次式

$$\Xi_S = \max_{\Delta x \neq 0, \Gamma y \neq 0} \xi_S(\Delta x, \Gamma y) \quad (15)$$

で表される最大値Ξ_sが差分線形攻撃指標となる。指標Ξ_sの値が大きいと差分線形攻撃における脆弱点となりうるため、この値が小さい（顕著な偏りがない）ことが差分線形攻撃に対して耐性を持つための必要条件となる。

ところで、次式

$$S: \quad GF(2)^n \rightarrow GF(2)^n: \quad x \rightarrow x^{2^k} \text{ in } GF(2^n) \qquad (16a)$$

$$S: \quad GF(2)^n \rightarrow GF(2)^n: \quad x \rightarrow x^{2^k+1} \text{ in } GF(2^n) \qquad (16b)$$

で示されるような関数Sは幾つかの暗号で用いられているが、kをn以下の自然数としたとき、これらの関数Sの差分線形攻撃指標は2^n（理論的最大値）をとる。この性質が具体的な暗号の攻撃に結びついた例はまだ報告されていないが、この指標がなるべく小さい値をとることが望ましい。

次に、この発明による第２の観点の実施例について述べる。

上述のようにして各種攻撃に対するS-box の耐性が評価されたが、耐性の強いランダム関数を生成するには、候補となる関数群をどのように選ぶかという問題点が生じる。膨大な関数の中から上記の条件を満たす関数を選ぶのには多くの計算量を必要とするためである。

ところで、文献「T. Jakobsen, L. R. Knudsen: “The Interpolation Attack on Block Cipher, ” Fast Software Encryption Workshop(FSE4) (Lecture Notes in Computer Science 1267), pp. 28-40, Springer Verlag , 1997」で挙げられている例により、差分解読法や線形解読法に対する耐性をもつ関数として、ある代数構造をもつ関数を選んでS-box として採用し、その代数構造を壊さない演算のみと組み合わせて暗号全体を構成すると、高階差分攻撃法や補間攻撃法などの代数攻撃法により容易に解読されることが分かっている。ところがこの出願の発明者らは、差分解読法及び線形解読法に対する耐性を有する関数と、その関数と異なる代数構造（基本演算構造）を有する関数とを組み合わせた合成関数は、その他の攻撃法に対しても耐性を有する関数となっている場合が多いことを見いだした。

そこで、この発明による第２の観点では、差分解読法及び線形解読法に対する耐性を持つ関数と、その関数の代数構造とは異なる代数構造を持つ関数を組み合わせた関数（例えば関数の合成など）を候補の関数群として選び、その関数群のそれぞ

れについてその各解読に対する耐性を評価し、耐性の強いものを選択する。

なお、この発明における候補関数群の選び方は必ずしも以上の手段に限定される必要はない。

この発明の第２の観点によれば差分解読法及び線形解読法に対する耐性をもつ少なくとも１つの関数と、その関数の代数構造と異なる代数構造をもつ少なくとも１つの関数を組み合わせた関数（例えば、合成関数）を候補の関数群として選ぶことで、少ない候補の中から、差分解読法や線形解読法だけでなく、高階差分攻撃法、補間攻撃法などの代数的構造を利用した攻撃法に対する耐性をもつ関数を効率的に絞り込むことができる。

以下、第２の観点による実施例では、S-box として８ビット入出力のS-box の設計法について述べる。

まず、S-box ２０を構成する候補関数として、例えば図２に示すように関数P(x, e)を生成するＰ関数部２１と、関数P(x, e)と代数構造を異にする関数A(y, a, b)を生成するＡ関数部２２とが合成されたものとする。

$$S : GF(2)^8 \rightarrow GF(2)^8 ; \quad x \mapsto A((P(x,e)),a,b)$$

但し

$$P(x,e) = x^e \ \text{in} \ GF(2^8) \qquad (17)$$

$$A(y,a,b) = ay+b \pmod{2^8} \qquad (18)$$

とする。式(17)で規定される関数P(x, e)はガロア体GF(2^8)上で定義されるべき乗関数であり、パラメータｅを適切に選ぶと差分解読法及び線形解読法に対し耐性を有しているが、高階差分攻撃、線形差分攻撃、補間攻撃、分割攻撃などに対しては耐性を有していない。一方、式(18)で規定される関数A(y, a, b)は単純な加算と乗算により構成され、いずれの攻撃に対しても耐性を有していない。

ここでは、パラメータａ，ｂ，ｅは０以上255（即ち2^8-1)以下の任意の自然数という自由度がある。このうち、パラメータａ，ｂのハミング重みを３以上５以下に限定し、つまりａ，ｂは各８ビットであるがそのうち"1"（又は"0"）が３ビット以上５ビット以下であり、更にS-box が全単射であること、差分解読法、線形解読法、高階差分攻撃法、補間攻撃法、分割攻撃法に対する耐性があるための必要条件を満

たすかどうかを評価し、パラメータａ，ｂ，ｅを絞り込んでいく。

その例、つまりこの発明の装置の一実施例の処理手順を図３に示す。なお、実施例はこの例に限られない。S-box の候補とする関数の選び方には自由度がある。またS-box の設計指標も数多くあり、その優先順位や候補関数の絞り込みの順序など、多くの自由度がある。

ステップＳ１：入力部１１で予め式(17),(18) におけるパラメータa, b, e の範囲を０以上2^8-1以下に決め、更にａ及びｂは、それらのハミング重みW_h(a) 及びW_h(b) を３以上５以下に限定する。

ステップＳ２：候補関数Ｓが全単射であるかを評価する。パラメータａが奇数、ｅが$2^8-1=255$と互いに素（ (e, 255)=1と表す）である時、関数Ｓは全単射になるので、これらを満たすパラメータを選択し、満たさないものは候補から除く。この処理は図１中のその他の指標評価部14g により行う。あるいはパラメータａは入力部１１で奇数のみを入力することで得る。

ステップＳ３：ｅのハミング重みW_h(e) （２進表現のｅ中の"1" の個数であり、例えばe=11101011であればW_h(e)=6 ） と関数Ｐのブール関数表現での次数deg_xＰとが等しいことが知られている。そこで、残りの候補関数Ｓの高階差分攻撃指標deg_xＳの条件を満たすため、ここではdeg_xＰ、つまりｅのハミング重みW_h(e) の理論的最大値である７になるもの、即ちe=127, 191, 223, 239, 251, 253, 254 を選択する。これを満たさないものは候補から除く。

ステップＳ４：選択した結果、候補が残ったか判定する。

ステップＳ５：ステップで候補がないと判定された場合、W_h(e)←W_h(e)-1と条件をゆるめてステップＳ３に戻る。

ステップＳ６：ステップＳ３の処理で残った候補の関数Ｓについて、式(3) で規定される差分攻撃指標Δ_s が予め決めた基準値Δ_R 以下となるものを選択する。これを満たさないものは候補から除く。

ステップＳ７：ステップＳ６の処理により候補が残ったか判定する。

ステップＳ８：候補が残らなかった場合、基準値Δ_R に予め決めたステップ幅Δ_d を加算する（条件をゆるめる）ことにより基準値Δ_R を更新し、ステップＳ６に

戻り、処理を繰り返す。

ステップＳ９：ステップＳ６の処理で残った候補関数Ｓについて、式(5) で規定される線形攻撃指標Λ_s が予め決めた基準値Λ_R 以下となるものを選択する。これを満たさないものは候補から除く。

ステップＳ１０：ステップＳ９の処理により候補が残ったか判定する。

ステップＳ１１：候補が残らなかった場合、基準値Λ_R に予め決めたステップ幅Λ_d を加算する（条件をゆるめる）ことにより基準値Λ_R を更新し、ステップＳ９に戻り、処理を繰り返す。

ステップＳ１２：ステップＳ９の処理で残った候補関数Ｓについて、式(15)で規定される差分線形攻撃指標Ξ_s が予め決めた基準値Ξ_R 以下となるものを選択する。これを満たさないものは候補から除く。

ステップＳ１３：ステップＳ１２の処理により候補が残ったか判定する。

ステップＳ１４：候補が残らなかった場合、基準値Ξ_R に予め決めたステップ幅Ξ_d を加算する（条件をゆるめる）ことによりΞ_R を更新し、ステップＳ１２に戻り、処理を繰り返す。

この結果、以下のパラメータまで絞り込める。

$(a, b) = (97, 97),\ (97, 225),\ (225, 97),\ (225, 225)$

$e = 127, 191, 223, 239, 247, 251, 253, 254$

ステップＳ１５：ステップＳ１２の処理で残った上記のパラメータの全ての組み合わせによる候補関数Ｓについて、分割攻撃指標$I_S(F, G)$ を求め、$|I_S(F, G)-1/2|$ が基準値I_R以下となるものを選ぶ。これを満たさないものは候補から除く。

ステップＳ１６：ステップＳ１５の処理により候補が残ったか判定する。

ステップＳ１７：候補が残らなかった場合、基準値I_Rに予め決めたステップ幅I_dを加算する（条件をゆるめる）ことにより基準値I_Rを更新し、ステップＳ１５に戻り、処理を繰り返す。

ステップＳ１８：ステップＳ１５の処理で残った上記パラメータの全ての組み合わせによる候補関数Ｓについて、GF(2^8)上の多項式を利用する補間攻撃指標$coeff_qS$（ただし$q = 2^8$）が基準値c_{qR} 以上となるものを選択し、それ以外を除去する。

ステップＳ１９：ステップＳ１８の処理により候補が残ったか判定する。

ステップＳ２０：候補が残らなかった場合、基準値c_{qR}から予め決めたステップ幅c_{qd}を減算する（条件をゆるめる）ことにより基準値I_Rを更新し、ステップＳ１９に戻り、処理を繰り返す。

ステップＳ２１：2^8+1以上2^9以下の全ての素数ｐについて、関数ＳのGF(p) 上の多項式を利用する補間攻撃指標$coeff_p S$が基準値c_{pR}以上となるものを選択し、それ以外を除去する。

ステップＳ２２：ステップＳ２１の処理により候補が残ったか判定する。

ステップＳ２３：候補が残らなかった場合、基準値c_{pR}から予め決めたステップ幅c_{pd}を減算する（条件をゆるめる）ことにより基準値c_{pR}を更新し、ステップＳ２１に戻り、処理を繰り返す。

以上の評価の結果、以下のパラメータの組み合わせ（全３２種類）が残る。

$$(a, b) = (97, 97), (97, 225), (225, 97), (225, 225)$$

$$e = 127, 191, 223, 239, 247, 251, 253, 254$$

この結果はステップＳ１２で得られた結果と同一である。つまりこの例ではステップＳ１２で既に本実施例で考慮するあらゆる攻撃法に対しても強い関数が得られたことになる。

このようにして選択された３２個の関数は上記の評価基準における強度は等しいので、S-box としてどの関数を選んでもよい。

S-box の評価として、又は関数生成において、各評価指標の基準値Δ_R，Λ_R，Ξ_R，c_{qR}，c_{pR}は、要求されるランダム性の程度、つまり各種の攻撃に対し要求される強さに応じて決定される。

図３の処理フローにおいて、それぞれの攻撃法（解読法）に対する要求された耐性を有する関数候補の選択順は、図３に示した順に限らず、他の順に実行してもよい。

この発明によるランダム関数生成方法では、図３に示した全ての攻撃法に対しそれぞれ要求された耐性を有する関数候補の選択を実行する必要はなく、少なくとも高階差分攻撃、差分線形攻撃、分割攻撃、補間攻撃の内の少なくとも１つについて

関数候補の選択を実行することもこの発明に含まれる。また、複数の解読法に対し順次関数候補の選択を実行して候補を絞っていく代わりに、全ての関数候補についてそれぞれの解読法に対する耐性評価を行い、それらの解読法に対し基準の耐性を満たすものを選択してもよい。

上述のランダム関数生成方法は、２つの関数の合成関数のパラメータを決定する場合を示したが、３つ以上の関数を組み合わせた関数のパラメータについても同様に適用できるし、また１つの関数のパラメータを決定する場合にも適用できることは言うまでもない。

上述した第１実施例及び第２実施例で説明したこの発明による関数のランダム性評価方法及びランダム関数生成方法をコンピュータで実施するプログラムとして記録媒体に予め記録しておけき、その記録媒体のプログラムをコンピュータで読み出して実行することにより関数のランダム性評価及びランダム関数の生成を実施してもよい。

発明の効果

以上述べたように、この発明によれば、暗号装置等の構成要素となるS-box 関数のランダム性評価方法及びその装置において、従来の評価方法に加えて、差分解読法、線形解読法、高階差分攻撃法、補間攻撃法、分割攻撃法、差分線形攻撃法その他想定される攻撃法に対する耐性をもつかどうか評価する手段を加えることで、ランダム性の評価を行え、かつ上記の暗号攻撃に対する高い安全性をもつ暗号が設計できる。

更に、候補となる関数群を差分解読法や線形解読法に対する耐性をもつ関数と、その関数の代数構造と異なる代数構造をもつ関数を組み合わせた関数を候補の関数群として選ぶことで、少ない候補の中から、差分解読法や線形解読法だけでなく、高階差分攻撃法、補間攻撃法などの代数的構造を利用した攻撃法に対する耐性をもつ関数を効率的に絞り込むことができる。

また図３に示したような手順で絞り込みを行うと、少ない演算量で効率的に絞り込みを行うことができる。

また、候補となる関数群をランダムに選ぶのではなく、よく知られた異なる代数

構造をもつ関数の組み合わせから選ぶことで、S-box にトラップドア（設計者だけがその暗号を解読できるような秘密のしかけ）がないことも示しやすい。

この発明によりこのようにして評価生成されたランダム関数は、高速かつ安全にデータを秘匿する暗号装置において、入力に対し不規則な出力を生成するS-boxとして、例えばＲＯＭにより構成するなどのように使用される。

請求の範囲

1．評価すべき関数の各出力ビットを入力ビットに関するブール多項式で表現したときの次数の最小値を求めてその最小値が大きいほど高階差分攻撃法に対する耐性が大であると評価する高階差分攻撃耐性評価手段と、

上記評価すべき関数に対し、鍵kを固定して入力をxとしたとき、素数p又はpのべき乗個の要素からなるガロア体上の多項式を用いて出力yを$y=f_k(x)$と表現して、上記多項式の項数を求め、その項数が大であるほど補間攻撃法に対する耐性が大であると評価する補間攻撃耐性評価手段と、

上記評価すべき関数の全ての入力xとそれらに対応する出力yをそれぞれ入力部分集合及び出力部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との関係の、その平均的対応関係に対する偏りを求めて、分割攻撃法に対する耐性を評価する分割攻撃耐性評価手段と、

評価すべき関数$S(x)$について入力差分Δxと出力マスク値Γyの全ての組に対し$(S(x)+S(x+\Delta x))$と出力のマスク値Γyとの内積が1であるxの個数を求めて差分線形攻撃法に対する耐性を評価する差分線形攻撃耐性評価手段と、

の少くとも1つの評価手段を含むことを特徴とする関数のランダム性評価装置。

2．請求項1のランダム性評価装置において、

上記分割攻撃耐性評価手段は、上記関数の入力集合Fと出力集合Gをそれぞれu個の入力部分集合$\{F_0, F_1, \ldots, F_{u-1}\}$とv個の出力部分集合$\{G_0, G_1, \ldots, G_{v-1}\}$に分割し、各分割対$(F_i, G_j)$$(i=0,\ldots,u-1; j=0,1,\ldots,v-1)$について入力部分集合$F_i$の全入力xに対応する全出力yがそれぞれの出力部分集合$G_j$$(j=0,\ldots,v-1)$へ帰属する確率のうちの最大値を求め、全ての分割対についての全ての最大値に基づいて分割対(F,G)の平均的偏りの指標$I_s(F,G)$を求め、分割攻撃法に対する耐性を評価する手段であり、

上記差分線形攻撃耐性評価手段は、出力マスク値をΓyとすると、0を除く入力差分Δxと0を除く出力マスク値Γyの全ての組について次式

$$\xi_s(\Delta x, \Gamma y) = |2\times\#\{x\in GF(2)^n \mid (S(x)+S(x+\Delta x))\cdot\Gamma y=1\}-2^n|$$

を計算し、計算結果の中で最大値Ξ_sを求め、上記Ξ_sを差分線形攻撃法に対する耐性を評価する手段である。

3．請求項1又は2記載の関数のランダム性評価装置において、

評価すべき関数S(x)について、全ての($\Delta x, \Delta y$)の組に対しS(x)+S(x+S(x+Δx)=Δyを満すxの個数を求めて差分解読法に対する耐性を評価する差分解読法耐性評価手段と、

評価すべき関数についてその入力xとそのマスク値Γxの内積が、関数出力値S(x)とそのマスク値Γyとの内積に等しくなるxの個数を求めて、線形解読法に対する耐性を評価する線形解読法耐性評価手段との少くとも1つを更に含む。

4．請求項3記載のランダム性評価装置において、上記線形解読法耐性評価手段は、$\Gamma y=0$ を除く全てのマスク値の組($\Gamma x, \Gamma y$) に対し次式

$$\lambda_s(\Gamma x, \Gamma y) = |2\times \#\{x\in GF(2)^n \mid x\cdot \Gamma x = S(x)\cdot \Gamma y\} - 2^n|$$

を求め、更に次式

$$\Lambda_s = \max \lambda_s(\Gamma x, \Gamma y)$$

で規定される指標により、線形解読法に対する耐性を評価する手段である。

5．請求項3記載のランダム性評価装置において、上記差分解読法耐性評価手段は、$\Delta x=0$ を除く全ての差分値の組($\Delta x, \Delta y$) に対し次式

$$\delta_s(\Delta x, \Delta y) = \#\{x\in GF(2)^n \mid S(x)+S(x+\Delta x) = \Delta y\}$$

を求め、更に次式

$$\Delta_s = \max \delta_s(\Delta x, \Delta y)$$

で規定される指標により、差分解読法に対する耐性を評価する手段である。

6．代数構造の異なる複数の関数を組合わせた関数であり複数のパラメータを有する候補関数群を生成する候補関数生成手段と、

上記各候補関数群のそれぞれについて、解読攻撃に対する耐性を評価する耐性評価手段と、

上記耐性評価された候補関数群から耐性の強いものを選出する選択手段と、

を含むランダム関数生成装置。

7．請求項6記載のランダム関数生成装置において、

上記代数構造の異なる関数の１つは差分解読法及び線形解読法に対する各耐性が強いものである。

８．請求項６又は７記載のランダム関数生成装置において、上記耐性評価手段は、

上記候補関数の各出力ビットを入力ビットに関するブール多項式で表現したときの次数の最小値を求めて高階差分攻撃法に対する耐性を評価する高階差分攻撃耐性評価手段と、

上記候補関数に対し、鍵ｋを固定してｘを入力としたとき、素数ｐ又はｐのべき乗個の要素からなるガロア体上の多項式を用いて出力ｙを$y=f_k(x)$と表現して、上記多項式の項数を求めて、補間攻撃法に対する耐性を評価する補間攻撃耐性評価手段と、

上記候補関数の全ての入力とそれらに対応する出力をそれぞれの部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との対応関係の、その平均的対応関係に対する偏りを求めて、分割攻撃法に対する耐性を評価する分割攻撃耐性評価手段と、

上記候補関数$S(x)$について全ての入力差分Δxと出力マスク値Γyの全ての組に対し、$(S(x)+S(x+\Delta x))$と出力のマスク値Γyとの内積が１であるｘの個数を求めて差分線形攻撃法に対する耐性を評価する差分線形攻撃耐性評価手段と、

の少くとも１つを含む。

９．関数の入出力関係のランダム性を評価する方法であり、

(a) 上記関数を$S(x)$とすると、上記関数$S(x)$の各出力ビットを入力ビットに関するブール多項式で表現したときの次数の最小値を求めて高階差分攻撃法に対する耐性を評価する高階差分攻撃耐性評価処理ステップと、

(b) 評価すべき関数$S(x)$について入力差分Δxと出力マスク値Γyの全ての組に対し$(S(x)+S(x+\Delta x))$と出力のマスク値Γyとの内積が１であるｘの個数を求めて差分線形攻撃法に対する耐性を評価する差分線形攻撃耐性評価処理ステップと、

(c) 上記評価すべき関数の全ての入力ｘとそれらに対応する出力ｙをそれぞれ入力部分集合及び出力部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との関係の、その平均的対応関係に対する偏りを求めて、分割攻撃法に対

する耐性を評価する分割攻撃耐性評価処理ステップと、

(d) 上記関数に対し、鍵kを固定してxを入力とし、素数p又はpのべき乗個の要素からなるガロア体上の多項式を用いて上記関数の出力yをを$y=f_k(x)$と表現して、上記多項式の項数により補間攻撃法に対する耐性を評価する補間攻撃耐性評価処理ステップ、

の少なくとも1つを含む。

10. 請求項9のランダム性評価方法において、

上記差分線形攻撃耐性評価処理ステップ(b) は上記関数S(x)の入力の差分をΔxとし、出力マスク値をΓyとすると、0を除く入力差分Δxと0を除く出力マスク値Γyの全ての組について次式

$$\xi_s(\Delta x, \Gamma y)=|2\times \#\{x\in GF(2)^n \mid (S(x)+S(x+\Delta x))\cdot \Gamma y=1\}-2^n|$$

を計算し、計算結果の中で最大値Ξ_sを求め、上記Ξ_sを差分線形攻撃法に対する耐性を評価するステップであり、

上記分割攻撃耐性評価処理ステップ(c) は上記関数の入力集合Fと出力集合Gをそれぞれu個の入力部分集合$\{F_0, F_1, \ldots, F_{u-1}\}$とv個の出力部分集合$\{G_0, G_1, \ldots, G_{v-1}\}$に分割し、各分割対$(F_i, G_j)$ $(i=0,\ldots,u-1; j=0,1,\ldots,v-1)$について入力部分集合$F_i$の全入力xに対応する全出力yがそれぞれの出力部分集合G_j $(j=0,\ldots,v-1)$へ帰属する確率を求め、全ての分割対(F, G) の帰属確率の偏りの指標$I_s(F, G)$を求め、その指標に基づいて分割攻撃法に対する耐性を評価するステップである。

11. 請求項9又は10のランダム性評価方法において、更に、

(e) 上記関数S(x)の出力差分値をΔyとすると、$\Delta x=0$を除く全ての差分値の組$(\Delta x, \Delta y)$に対し$S(x)+S(x+\Delta x)=\Delta y$を満すxの個数をそれぞれ求め、それらのうちの最大値により差分解読法に対する耐性を評価する差分解読法耐性評価処理ステップと、

(f) 上記関数S(x)についてその入力xとそのマスク値Γxの内積が、関数出力値S(x)とそのマスク値Γyとの内積に等しくなるxの個数を求めて、線形解読法に対する耐性を評価する線形解読法耐性評価処理ステップ、

との少くとも１つを更に含む。

１２．請求項１１のランダム性評価方法において、上記入力ｘのビット数をｎとすると、

上記差分解読法耐性評価処理ステップ(e) は、Δx=0 を除く全ての差分値の組(Δx, Δy) に対しそれぞれ次式

$$\delta_s(\Delta x, \Delta y) = \#\{x \in GF(2)^n \mid S(x)+S(x+\Delta x) = \Delta y\}$$

を求め、更に次式

$$\Delta_s = \max \ \delta_s(\Delta x, \Delta y)$$

で規定される指標Δ_s により、差分解読法に対する耐性を評価する処理ステップであり、

上記線形解読法耐性評価処理ステップ(f) は、上記入力ｘのマスク値をΓx とすると、$\Gamma y=0$ を除く全ての組のマスク値($\Gamma x, \Gamma y$) に対し次式

$$\lambda_s(\Gamma x, \Gamma y) = |2\times \#\{x \in GF(2)^n \mid x \cdot \Gamma x = S(x) \cdot \Gamma y\} - 2^n|$$

を求め、更に次式

$$\Lambda_s = \max \ \lambda_s(\Gamma x, \Gamma y)$$

で規定される指標Λ_s により、線形解読法に対する耐性を評価する処理ステップである。

１３．ランダム関数生成方法であり、以下の処理ステップを含む：

(a) 候補関数について、各パラメータに各種値を設定し、各種入力値に対する出力値をそれぞれ演算する演算処理ステップと、

(b) 上記演算処理の結果を記憶手段に記憶する処理ステップと、

(c) 上記記憶手段に記憶された値を用いて上記各候補関数のそれぞれについて、解読攻撃に対する耐性を評価し、その耐性評価結果にもとづき、耐性の強い候補関数を選択出力する選択処理ステップと、

を含み、上記処理ステップ(c) は以下の少なくとも１つのステップを含む：

(c-1) 上記候補関数の各出力ビットを入力ビットに関するブール多項式で表現したときの次数の最小値を求めて高階差分攻撃法に対する耐性を評価し、耐性が予め決めた第１の基準より強い候補関数を残し他を除去する高階差分攻撃耐性評価

選択処理ステップと、

(c-2) 各候補関数S(x)について入力差分Δx と出力マスク値Γy の全ての組(Δx, Γy) に対しそれぞれS(x)+S(x+Δx) と出力のマスク値Γy との内積が１であるｘの個数を求めて差分線形攻撃法に対する耐性を評価し、耐性が予め決めた第２の基準より強い候補関数を残し、他を除去する差分線形攻撃耐性評価処理ステップと、

(c-3) 各候補関数の全ての入力とそれらに対応する出力をそれぞれの部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との対応関係の、その平均的対応関係に対する偏りを求めて、分割攻撃法に対する耐性を評価し、耐性が予め決めた第３の基準より強い候補関数を残し、他を除去する分割攻撃耐性評価処理ステップと、

(c-4) 候補関数に対し、鍵ｋを固定してｘを入力とし、素数ｐ又はｐのべき乗個の要素からなるガロア体上の多項式を用いて出力ｙをy＝$f_k(x)$と表現して、上記多項式の項数を求めて補間攻撃法に対する耐性を評価し、耐性が予め決めた第４の基準より強い候補関数を残して他を除去する補間攻撃耐性評価処理ステップ。

１４．請求項１３のランダム関数生成装置において、

上記差分線形攻撃耐性評価処理ステップ(c-2) は、出力マスク値をΓy とすると、０を除く入力差分Δx と０を除く出力マスク値Γy の全ての組について次式

$$\xi_s(\Delta x, \Gamma y) = |2\times \#\{x\in GF(2)^n \mid (S(x)+S(x+\Delta x))\cdot \Gamma y=1\} - 2^n|$$

を計算し、計算結果の中で最大値Ξs を求め、上記Ξs を差分線形攻撃法に対する耐性を評価するステップを含み、

上記分割攻撃耐性評価処理ステップ(3) は、上記関数の入力集合Ｆと出力集合Ｇをそれぞれｕ個の入力部分集合 $\{F_0, F_1, \ldots, F_{u-1}\}$ とｖ個の出力部分集合 $\{G_0, G_1, \ldots, G_{v-1}\}$ に分割し、各分割対(F_i, G_j)(i=0,...,u-1; j=0,1,...,v-1)について入力部分集合F_iの全入力ｘに対応する全出力ｙがそれぞれの出力部分集合G_j(j=0,...,v-1) へ帰属する確率のうちの最大値を求め、全ての分割対についての全ての最大値に基づいて分割対(F, G) の平均的偏りの指標Is(F, G) を求め、分割攻撃法に対する耐性を評価するステップを含む。

１５．請求項１３又は１４のランダム関数生成方法において、

上記ステップ(c-1) は、候補関数が残らなかった場合は、上記第１の基準を第１の所定幅だけ変化させることにより選択条件をゆるめて評価選択処理を再度実行するステップを含み、

上記ステップ(c-2) は、候補関数が残らなかった場合は、上記第２の基準を第２の所定幅だけ変化させることにより選択条件をゆるめて評価選択処理を再度実行するステップを含み、

上記ステップ(c-3) は、候補関数が残らなかった場合は、上記第３の基準を第３の所定幅だけ変化させることにより選択条件をゆるめて評価選択処理を再度実行するステップを含み、

上記ステップ(c-4) は、候補関数が残らなかった場合は、上記第４の基準を第４の所定幅だけ変化させることにより選択条件をゆるめて評価選択処理を再度実行するステップを含む。

１６．請求項１３又は１４のランダム関数生成方法は更に以下の少なくとも１つのステップを含む：

(c-5) 候補関数S(x)について、$\Delta x=0$ を除く全ての組(Δx, Δy)に対しS(x)+S(x+Δx)＝Δyを満すｘの個数をそれぞれ求め、それらのうちの最大値により差分解読法に対する耐性を評価し、耐性が予め決めた第５の基準より強い候補関数を残し、他を除去する差分解読法耐性評価処理ステップと、

(c-6) 各候補関数についてその入力ｘとそのマスク値Γx の内積が、関数出力値S(x)とそのマスク値Γy との内積と等しくなる全てのｘの個数を全ての組の(Γx, Γy) について求め、それらに基づいて線形解読法に対する耐性を評価し、耐性が予め決めた第６の基準より強い候補関数を残し、他を除去する線形解読法耐性評価処理ステップ。

１７．請求項１６のランダム関数生成方法において、上記差分解読法耐性評価処理ステップ(c-5) は、$\Gamma y=0$ を除く全ての差分値の組(Δx, Δy) に対し次式

$$\delta_s(\Delta x, \Delta y) = \#\{x \in GF(2)^n \mid S(x)+S(x+\Delta x) = \Delta y\}$$

を求め、更に次式

$$\Delta_s = \max \ \delta_s(\Delta x, \Delta y)$$

で規定される指標により、差分解読法に対する耐性を評価するステップを含み、

上記線形解読法耐性評価処理ステップ(c-6) は、全てのマスク値の組(Γx, Γy) に対し次式

$$\lambda_s(\Gamma x, \Gamma y) = |2 \times \#\{x \in GF(2)^n \mid x \cdot \Gamma x = S(x) \cdot \Gamma y\} - 2^n|$$

を求め、更に次式

$$\Lambda_s = \max \lambda_s(\Gamma x, \Gamma y)$$

で規定される指標により、線形解読法に対する耐性を評価するステップを含む。

１８．請求項１６又は１７のランダム関数生成方法において、

上記ステップ(c-5) は候補関数が残らなかった場合は、上記第５基準を第５の所定幅だけ変化させることにより選択条件をゆるめて評価選択を再度実行するステップを含み、

上記ステップ(c-6) は候補関数が残らなかった場合は、上記第６基準を第６の所定幅だけ変化させることにより選択条件をゆるめて評価選択を再度実行するステップを含む。

１９．請求項１３、１４又は１５のいずれかのランダム関数生成方法において、上記候補関数は差分解読法と線形解読法に対する耐性を有する少なくとも１つの関数と、上記関数と代数構造の異なる少なくとも１つの関数との合成関数である。

２０．ランダム関数生成方法をコンピュータプログラムとして記録した記録媒体であり、上記プログラムは以下の処理ステップを含む：

(a) 候補関数について、各パラメータに各種値を設定し、各種入力値に対する出力値をそれぞれ演算する演算処理ステップと、

(b) 上記演算処理の結果を記憶手段に記憶する処理ステップと、

(c) 上記記憶手段に記憶された値を用いて上記各候補関数のそれぞれについて、解読攻撃に対する耐性を評価し、その耐性評価結果にもとづき、耐性の強い候補関数を選択出力する選択処理ステップと、

を含み、上記処理ステップ(c) は以下の少なくとも１つのステップを含む：

(c-1) 上記候補関数の各出力ビットを入力ビットに関するブール多項式で表現したときの次数の最小値を求めて高階差分攻撃法に対する耐性を評価し、耐性が予

め決めた第１の基準より強い候補関数を残し他を除去する高階差分攻撃耐性評価選択処理ステップと、

(c-2) 各候補関数S(x)について入力差分Δx と出力マスク値Γy の全ての組(Δx, Γy) に対しそれぞれS(x)+S(x+Δx) と出力のマスク値Γy との内積が１であるｘの個数を求めて差分線形攻撃法に対する耐性を評価し、耐性が予め決めた第２の基準より強い候補関数を残し、他を除去する差分線形攻撃耐性評価処理ステップと、

(c-3) 各候補関数の全ての入力とそれらに対応する出力をそれぞれの部分集合に分割し、入力が属する部分集合と、出力が属する部分集合との対応関係の、その平均的対応関係に対する偏りを求めて、分割攻撃法に対する耐性を評価し、耐性が予め決めた第３の基準より強い候補関数を残し、他を除去する分割攻撃耐性評価処理ステップと、

(c-4) 候補関数に対し、鍵ｋを固定してｘを入力とし、素数ｐ又はｐのべき乗個の要素からなるガロア体上の多項式を用いて出力ｙをy＝f_k(x)と表現して、上記多項式の項数を求めて補間攻撃法に対する耐性を評価し、耐性が予め決めた第４の基準より強い候補関数を残して他を除去する補間攻撃耐性評価処理ステップ。

２１．請求項２０の記録媒体において、

上記差分線形攻撃耐性評価処理ステップ(c-2) は、出力マスク値をΓy とすると、０を除く入力差分Δx と０を除く出力マスク値Γy の全ての組について次式

$$\xi_s(\Delta x, \Gamma y) = | 2\times \#\{x\in GF(2)^n \mid (S(x)+S(x+\Delta x))\cdot \Gamma y=1\} - 2^n |$$

を計算し、計算結果の中で最大値Ξs を求め、上記Ξs を差分線形攻撃法に対する耐性を評価するステップを含み、

上記分割攻撃耐性評価処理ステップ(3) は、上記関数の入力集合Ｆと出力集合Ｇをそれぞれｕ個の入力部分集合 {F_0, F_1, ..., F_{u-1} } とｖ個の出力部分集合 {G_0, G_1, ..., G_{v-1} } に分割し、各分割対(F_i, G_j) (i=0, ..., u-1; j=0, 1, ..., v-1)について入力部分集合F_iの全入力ｘに対応する全出力ｙがそれぞれの出力部分集合G_j (j=0, ..., v-1) へ帰属する確率のうちの最大値を求め、全ての分割対についての全ての最大値に基づいて分割対(F, G) の偏りの指標Is(F, G) を求め、分割攻撃法に対する耐性を評価するステップを含む。

２２．請求項２０又は２１の記録媒体において、

上記ステップ(c-1) は、候補関数が残らなかった場合は、上記第１の基準を第１の所定幅だけ変化させることにより選択条件をゆるめて評価選択処理を再度実行するステップを含み、

上記ステップ(c-2) は、候補関数が残らなかった場合は、上記第２の基準を第２の所定幅だけ変化させることにより選択条件をゆるめて評価選択処理を再度実行するステップを含み、

上記ステップ(c-3) は、候補関数が残らなかった場合は、上記第３の基準を第３の所定幅だけ変化させることにより選択条件をゆるめて評価選択処理を再度実行するステップを含み、

上記ステップ(c-4) は、候補関数が残らなかった場合は、上記第４の基準を第４の所定幅だけ変化させることにより選択条件をゆるめて評価選択処理を再度実行するステップを含む。

２３．請求項２０又は２１の記録媒体において、上記プログラムは更に以下の少なくとも１つの処理ステップを含む：

(c-5) 候補関数S(x)について、$\Delta x=0$ を除く全ての組(Δx, Δy)に対しS(x)+S(x+Δx)＝Δyを満すｘの個数をそれぞれ求め、それらのうちの最大値により差分解読法に対する耐性を評価し、耐性が予め決めた第５の基準より強い候補関数を残し、他を除去する差分解読法耐性評価処理ステップと、

(c-6) 各候補関数についてその入力ｘとそのマスク値Γx の内積が、関数出力値S(x)とそのマスク値Γy との内積と等しくなる全てのｘの個数を全ての組の(Γx, Γy) について求め、それらに基づいて線形解読法に対する耐性を評価し、耐性が予め決めた第６の基準より強い候補関数を残し、他を除去する線形解読法耐性評価処理ステップ。

２４．請求項２３の記録媒体において、上記差分解読法耐性評価処理ステップ(c-5) は、$\Delta x=0$ を除く全ての差分値の組(Δx, Δy) に対し次式

$$\delta_s(\Delta x, \Delta y) = \#\{x \in GF(2)^n \mid S(x)+S(x+\Delta x) = \Delta y\}$$

を求め、更に次式

$$\Delta_s = \max \ \delta_s(\Delta x, \Delta y)$$

で規定される指標により、差分解読法に対する耐性を評価するステップを含み、

上記線形解読法耐性評価処理ステップ(c-6) は、$\Gamma y=0$ を除く全てのマスク値の組$(\Gamma x, \Gamma y)$ に対し次式

$$\lambda_s(\Gamma x, \Gamma y) = |2\times \#\{x\in GF(2)^n \mid x\cdot \Gamma x = S(x)\cdot \Gamma y\} - 2^n|$$

を求め、更に次式

$$\Lambda_s = \max \ \lambda_s(\Gamma x, \Gamma y)$$

で規定される指標により、線形解読法に対する耐性を評価するステップを含む。

２５．請求項２３又は２４の記録媒体において、

上記ステップ(c-5) は候補関数が残らなかった場合は、上記第５基準を第５の所定幅だけ変化させることにより選択条件をゆるめて評価選択を再度実行するステップを含み、

上記ステップ(c-6) は候補関数が残らなかった場合は、上記第６基準を第６の所定幅だけ変化させることにより選択条件をゆるめて評価選択を再度実行するステップを含む。

２６．請求項２０、２１又は２２のいずれかの記録媒体において、上記候補関数は差分解読法と線形解読法に対する耐性を有する少なくとも１つの関数と、上記関数と代数構造の異なる少なくとも１つの関数との合成関数である。

２７．関数の入出力関係のランダム性を評価する方法をプログラムとして記録した記録媒体であり、上記プログラムは以下の少なくとも１つの処理ステップを含む：

(a) 上記関数をS(x)とすると、上記関数S(x)の各出力ビットを入力ビットに関するブール多項式で表現したときの次数の最小値を求めて高階差分攻撃法に対する耐性を評価する高階差分攻撃耐性評価処理ステップと、

(b) 評価すべき関数S(x)について入力差分Δx と出力マスク値Γy の全ての組に対し$(S(x)+S(x+\Delta x))$と出力のマスク値Γy との内積が１であるｘの個数を求めて差分線形攻撃法に対する耐性を評価する差分線形攻撃耐性評価処理ステップと、

(c) 上記評価すべき関数の全ての入力ｘとそれらに対応する出力ｙをそれぞれ入力部分集合及び出力部分集合に分割し、入力が属する部分集合と、出力が属する

部分集合との関係の、その平均的対応関係に対する偏りを求めて、分割攻撃法に対する耐性を評価する分割攻撃耐性評価処理ステップと、

(d) 上記関数に対し、鍵kを固定してxを入力とし、素数p又はpのべき乗個の要素からなるガロア体上の多項式を用いて上記関数の出力yをを$y=f_k(x)$と表現して、上記多項式の項数により補間攻撃法に対する耐性を評価する補間攻撃耐性評価処理ステップ。

２８．請求項２７の記録媒体において、

上記差分線形攻撃耐性評価処理ステップ(b) は上記関数S(x)の入力の差分をΔxとし、出力マスク値をΓyとすると、0を除く入力差分Δxと0を除く出力マスク値Γyの全ての組について次式

$$\xi_s(\Delta x, \Gamma y) = |2\times \#\{x\in GF(2)^n \mid (S(x)+S(x+\Delta x))\cdot \Gamma y=1\} - 2^n|$$

を計算し、計算結果の中で最大値Ξ_sを求め、上記Ξ_sを差分線形攻撃法に対する耐性を評価するステップであり、

上記分割攻撃耐性評価処理ステップ(c) は上記関数の入力集合Fと出力集合Gをそれぞれu個の入力部分集合$\{F_0, F_1, \ldots, F_{u-1}\}$とv個の出力部分集合$\{G_0, G_1, \ldots, G_{v-1}\}$に分割し、各分割対$(F_i, G_j)$ $(i=0,\ldots,u-1; j=0,1,\ldots,v-1)$について入力部分集合$F_i$の全入力xに対応する全出力yがそれぞれの出力部分集合G_j $(j=0,\ldots,v-1)$へ帰属する確率を求め、全ての分割対(F, G) の帰属確率の平均的偏りの指標$I_s(F,G)$を求め、その指標に基づいて分割攻撃法に対する耐性を評価するステップである。

２９．請求項２７又は２８の記録媒体において、上記プログラムは更に、

(e) 上記関数S(x)の出力差分値をΔyとすると、$\Delta x=0$を除く全ての差分値の組$(\Delta x, \Delta y)$に対し$S(x)+S(x+\Delta x)=\Delta y$を満すxの個数をそれぞれ求め、それらのうちの最大値により差分解読法に対する耐性を評価する差分解読法耐性評価処理ステップと、

(f) 上記関数S(x)についてその入力xとそのマスク値Γxの内積が、関数出力値S(x)とそのマスク値Γyとの内積に等しくなるxの個数を求めて、線形解読法に対する耐性を評価する線形解読法耐性評価処理ステップ、

との少くとも１つを更に含む。

３０．請求項２９の記録媒体において、上記入力ｘのビット数をｎとすると、

上記差分解読法耐性評価処理ステップ(e) は、Δx=0 を除く全ての差分値の組(Δx, Δy) に対しそれぞれ次式

$$\delta_s(\Delta x, \Delta y) = \#\{x \in GF(2)^n \mid S(x)+S(x+\Delta x) = \Delta y\}$$

を求め、更に次式

$$\Delta_s = \max \ \delta_s(\Delta x, \Delta y)$$

で規定される指標Δ_s により、差分解読法に対する耐性を評価する処理ステップであり、

上記線形解読法耐性評価処理ステップ(f) は、上記入力ｘのマスク値をΓx とすると、$\Gamma y=0$ を除く全ての組のマスク値($\Gamma x, \Gamma y$) に対し次式

$$\lambda_s(\Gamma x, \Gamma y) = |\, 2\times \#\{x \in GF(2)^n \mid x \cdot \Gamma x = S(x) \cdot \Gamma y\} - 2^n \,|$$

を求め、更に次式

$$\Lambda_s = \max \ \lambda_s(\Gamma x, \Gamma y)$$

で規定される指標Λ_s により、線形解読法に対する耐性を評価する処理ステップである。

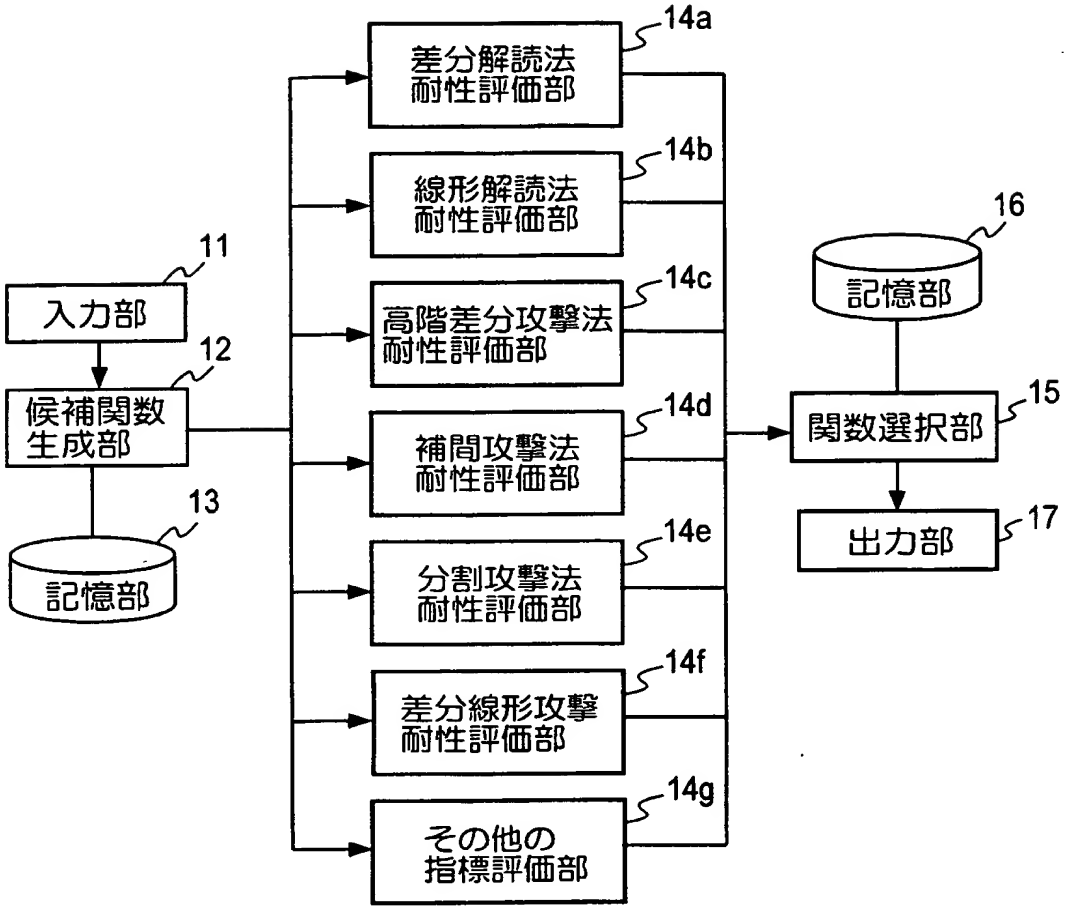

差分解読法
耐性評価部
14a
線形解読法
耐性評価部
14b
高階差分攻撃法
耐性評価部
14c
補間攻撃法
耐性評価部
14d
分割攻撃法
耐性評価部
14e
差分線形攻撃
耐性評価部
14f
その他の
指標評価部
14g
入力部
11
候補関数
生成部
12
記憶部
13
記憶部
16
関数選択部
15
出力部
17

図1

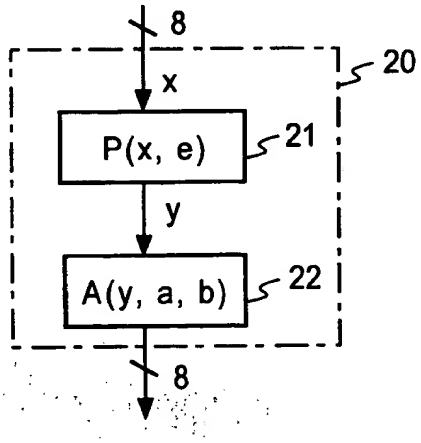
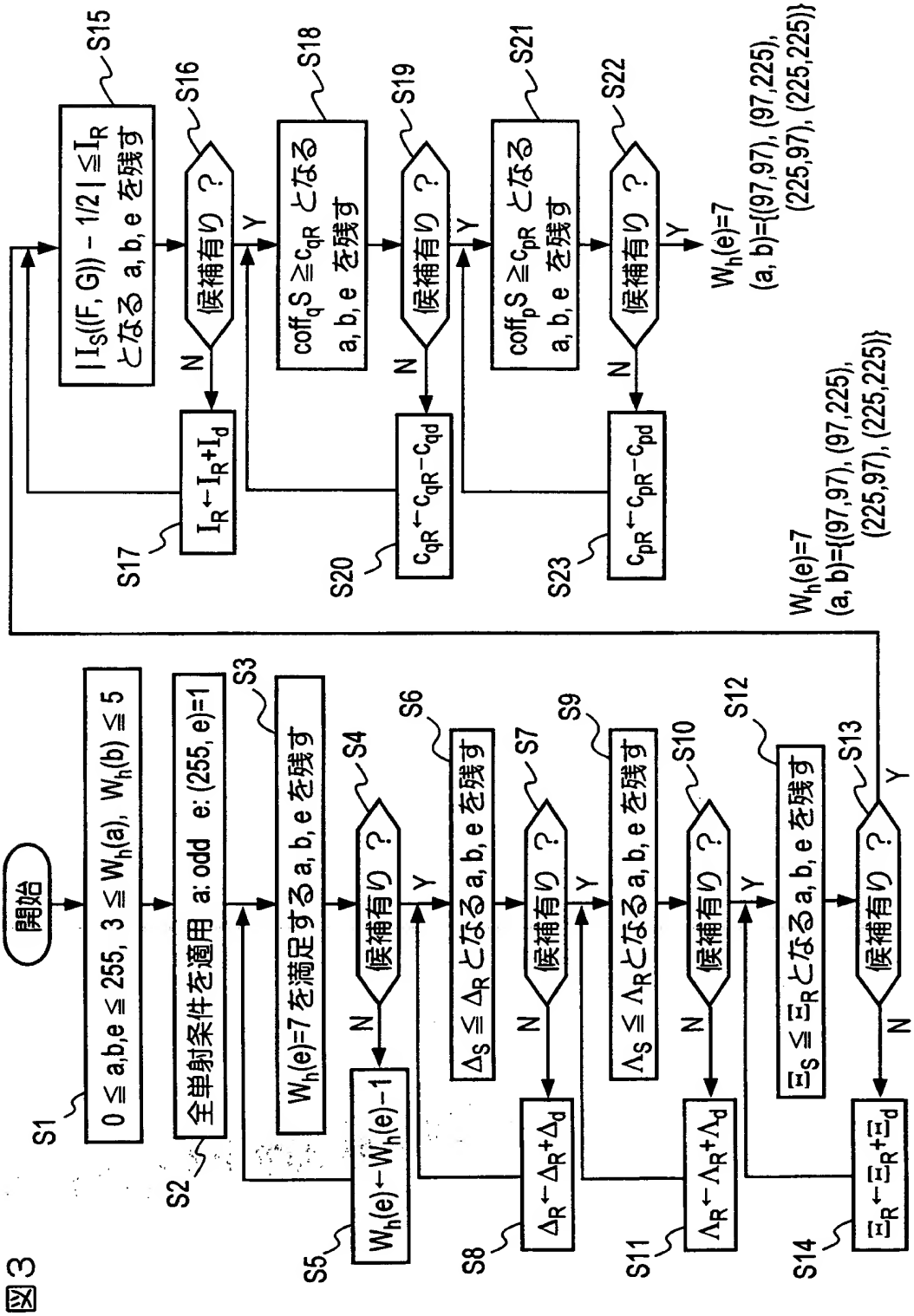

8
x
P(x, e)
21
y
A(y, a, b)
22
8
20

図2

図3


開始
S1
0 ≦ a,b,e ≦ 255, 3 ≦ Wh(a), Wh(b) ≦ 5
S2
全単射条件を適用 a: odd e: (255, e)=1
S3
Wh(e)=7 を満足する a, b, e を残す
S4
候補有り ？
N
Y
S5
Wh(e)←Wh(e)−1
S6
ΔS ≦ ΔR となる a, b, e を残す
S7
候補有り ？
N
Y
S8
ΔR←ΔR+Δd
S9
ΛS ≦ ΛR となる a, b, e を残す
S10
候補有り ？
N
Y
S11
ΛR←ΛR+Λd
S12
ΞS ≦ ΞR となる a, b, e を残す
S13
候補有り ？
N
Y
S14
ΞR←ΞR+Ξd
Wh(e)=7
(a, b)={(97,97), (97,225), (225,97), (225,225)}
S15
| IS((F, G)) − 1/2 | ≦ IR となる a, b, e を残す
S16
候補有り ？
N
Y
S17
IR←IR+Id
S18
coffqS ≧ cqR となる a, b, e を残す
S19
候補有り ？
N
Y
S20
cqR←cqR−cqd
S21
coffpS ≧ cpR となる a, b, e を残す
S22
候補有り ？
N
Y
S23
cpR←cpR−cpd
Wh(e)=7
(a, b)={(97,97), (97,225), (225,97), (225,225)}

This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/02924

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] H04L9/06, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G09C1/00-5/00, H04K1/00-3/00, H04L9/00-9/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Shiho Moriai, "Sabun/senkei/koukaisabun/hokan kougeki ni taishite tsuyoi S-box no ichi kouseihou", 1998 Nen Angou To Jouhou Security Symposium, (1998 January), SCIS'98-2.2.C	1-5, 9, 11, 12, 27, 29-30 6-8, 10, 13-26 28
X Y	Takeshi Hamada, Naofumi Yokoyama, Tooru Shimada, Toshinobu Kaneko, "Des angou ni taisuru partitioning kaiseki ni kansuru ichikousatsu", 1998 Nen Angou To Jouhou Security Symposium, (1998 January), SCIS'98-2.2.A	1, 3, 4, 9-12, 27-30 2, 5-8, 13-26
X Y	Susan K. Kangford and Martin E. Hellman, "Differential-Linear Cryptanalysis," Lecture Notes in Computer Science, Vol. 839, (1994), p.17-25	1-5, 9-12, 27-30 6-8, 13-26
Y	Kouichi Sakurai, "Angou riron no kiso", Kyoritsu Shuppan, (1996), p.69-72, particularly refer to page 72	6-8, 19, 26

[x] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 August, 1999 (12. 08. 99)	24 August, 1999 (24. 08. 99)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/02924

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Masatou Kanda, Youichi Takashima, Tsutomu Matsumoto, "Shousuu no S-box o mochiita round kansuu no kouseihou ni tsuite (sono 2)", 1998 Nen Angou To Jouhou Security Symposium, (1998 January), SCIS'98-2.2.D	6-8, 13-26
PX	Shiho Moriai Kazumaro Aoki, Masatou Kanda, Youichi Takashima, Kazuo Oota, "Kichi no block angou kougeki ni taisuru anzensei o kouryoshita S-box no kouseihou", Denshi Jouhou Tsuushin Gakkai Gijutsu Kenkyuu Houkoku, Vol. 98, No. 227, (30 July, 1998), p.25-32 (ISEC98-13)	1-30

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９９／０２９２４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int.Cl[6]　Ｈ０４Ｌ　９／０６
　　Ｇ０９Ｃ　１／００

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int.Cl[6]　Ｇ０９Ｃ　１／００　－　５／００
　　Ｈ０４Ｋ　１／００　－　３／００
　　Ｈ０４Ｌ　９／００　－　９／３８

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	盛合志帆“差分/線形/高階差分/補間攻撃に対して強いS-boxの一構成法”１９９８年暗号と情報セキュリティシンポジウム，（１９９８年１月），SCIS'98-2.2.C	1-5, 9, 11, 12, 27, 29-30 6-8, 10, 13-26, 28
X Y	浜田猛，横山尚史，島田徹，金子敏信“DES暗号に対するpartitioning解析に関する一考察”１９９８年暗号と情報セキュリティシンポジウム，（１９９８年１月），SCIS'98-2.2.A	1, 3, 4, 9-12, 27-30 2, 5-8, 13-26

[x] Ｃ欄の続きにも文献が列挙されている。　　[ ] パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 １２．０８．９９	国際調査報告の発送日　24.08.99
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 丸山　高政　　5W　9570 電話番号　０３－３５８１－１１０１　内線　３５７６

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ９９／０２９２４

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	Susan K. Kangford and Martin E. Hellman, "Differential-Linear Cryptanalysis," Lecture Notes in Computer Science, Vol.839, (1994), p.17-25	1-5,9-12, 27-30 6-8,13-26
Y	櫻井幸一「暗号理論の基礎」共立出版，（１９９６年），p.69-72，特に72ページ参照	6-8,19,26
A	神田雅透，高嶋洋一，松本勉"少数のS-boxを用いたラウンド関数の構成法について（その２）"１９９８年暗号と情報セキュリティシンポジウム，（１９９８年１月），SCIS'98-2.2.D	6-8,13-26
ＰＸ	盛合志穂，青木和麻呂，神田雅透，高嶋洋一，太田和夫 "既知のブロック暗号攻撃に対する安全性を考慮したS-boxの構成法" 電子情報通信学会技術研究報告，Vol.98，No.227，（１９９８年７月３０日），p.25－32（ISEC98-13）	1-30